IN THE CLAIMS

Please cancel claims 1-5 and substitute the following new claims 6-10.

What is claimed is:

1   1. (cancelled) ~~A wide area network using the internet as a backbone, comprising:~~

2   ~~a first dedicated line coupled to a first participating ISX/ISP provider of~~

3   ~~internet access;~~

4   ~~a source router having a channel service unit having an output coupled to~~

5   ~~said first dedicated line;~~

6   ~~a source firewall circuit having a first port for coupling directly or through a~~

7   ~~local area network to a first device for which communication over said wide area~~

8   ~~network (hereafter WAN) is desired, and having a WAN interface coupled to said~~

9   ~~source router directly or through a local area network, said source firewall functioning~~

10   ~~to encrypt the payloads of downstream WAN packets being transmitted via the WAN~~

11   ~~interface to said source router using any encryption method having a user definable~~

12   ~~key or keys, and for decrypting the payloads of any incoming upstream WAN packets~~

13   ~~arriving from said source router via said WAN interface using the same encryption~~

14   ~~method and user definable key or keys that were used to encrypt the outgoing WAN~~

15   ~~packets;~~

16   ~~one or more routers of other participating ISX/ISP providers of internet~~

17   ~~services including a router at an endpoint participating ISX/ISP provider, said routers~~

18   ~~functioning to implement a predetermined private tunnel data path coupling a router~~

19   ~~of said first ISX/ISP to a router of said endpoint participating ISX/ISP provider~~

20   ~~through said routers of said participating ISX/ISP providers;~~

21   ~~a destination router including a channel service unit coupled to or part of said~~

22   ~~destination router, said destination router coupled through said channel service unit~~

23   ~~and a second dedicated line to said router of said endpoint ISX/ISP provider;~~

24   ~~a destination firewall circuit having a WAN interface coupled to said~~

25   ~~destination router directly or through a local area network and having a second port~~

26   ~~for coupling directly or through a local area network to a device for which~~

27   ~~communication across said wide area network is desired, said firewall functioning to~~

28   ~~encrypt the payloads of upstream WAN packets being transmitted through said WAN~~

29   ~~interface to said destination router for transmission to said source router via said~~

30   ~~private tunnel using the same encryption method used by said source firewall and the~~

31   ~~same user definable key or keys used by said source firewall circuit, and for~~

32   ~~decrypting any incoming packets from said source router arriving from said endpoint~~

33   ~~participating ISX/ISP provider using the same encryption protocol used by said~~
34   ~~source firewall and the same user definable key or keys used by said source firewall~~
35   ~~circuit and transmitting the decrypted packets to said second device.~~

1   2.   (cancelled) ~~A process for launching downstream AlterWAN packets addressed to~~
2   ~~an AlterWAN destination into a private tunnel coupling two AlterWAN destinations using the~~
3   ~~internet as a backbone and for launching non-AlterWAN packets into a normal internet traffic~~
4   ~~routing data path, comprising the steps:~~
5   ~~receiving at a source firewall an incoming downstream wide area network~~
6   ~~packet from a workstation or other device at a first customer location said incoming~~
7   ~~downstream wide area network packet being either addressed to an AlterWAN~~
8   ~~destination or not an AlterWAN packet;~~
9   ~~at said source firewall, using the destination address in said incoming~~
10   ~~downstream wide area network packet to determine if said packet is addressed to an~~
11   ~~AlterWAN destination coupled to said source firewall by a private tunnel using the~~
12   ~~internet as a backbone (hereafter referred to as an AlterWAN packet) or is addressed~~
13   ~~to some non-AlterWAN website or location on the internet (hereafter referred to as a~~
14   ~~non-AlterWAN packet);~~
15   ~~if said packet is an AlterWAN packet, encrypting at said source firewall the~~
16   ~~payload portion thereof and forwarding the encrypted AlterWAN packet to a source~~
17   ~~router;~~
18   ~~if said packet is a non-AlterWAN packet, at said source firewall, forwarding~~
19   ~~said non-AlterWAN packet to said source router without encrypting the payload~~
20   ~~portion thereof;~~
21   ~~at said source router, converting both said AlterWAN packets and said non-~~
22   ~~AlterWAN packets into signals suitable for transmission on a dedicated telephone line~~
23   ~~or other transmission medium coupling said source router to a specially selected first~~
24   ~~ISX/ISP provider and transmitting said signals to said specially selected ISX/ISP~~
25   ~~provider, said specially selected ISX/ISP provider being selected either because their~~
26   ~~routing tables are such that AlterWAN packets will naturally be routed along high~~
27   ~~bandwidth, low hop count data paths to the next ISX/ISP provider in said virtual~~
28   ~~private network or because the routing tables of the router of said first ISX/ISP~~
29   ~~provider have been altered to insure that AlterWAN packets get routed along high~~
30   ~~bandwidth, low hop count data paths to the next ISX/ISP provider along said private~~
31   ~~tunnel.~~

1   3. (Cancelled) An apparatus comprising:

2   a dedicated data path for coupling to a specially selected first participating

3   ISX/ISP provider of internet access;

4   a firewall circuit having a first port for coupling directly or through a local area

5   network to one or more devices for which communication over a wide area network

6   using the internet as a backbone is desired, and having a second port, said firewall

7   functioning to to use the destination addresses in the headers of each packet

8   received from said one or more devices to distinguish between AlterWAN packets

9   which are packets addressed to destination devices coupled to said firewall circuit via

10   a private tunnel through the internet, and conventional packets which are packets

11   not addressed to destination devices coupled to said firewall circuit via a private

12   tunnel through the internet, said firewall circuit functioning to encrypt the payloads of

13   outgoing AlterWAN packets using one or more predetermined keys and an encryption

14   algorithm, and sending said encrypted AlterWAN packets to said source router via

15   said second port, and functioning to forward any conventional packets to said source

16   router, and functioning to decrypt any incoming AlterWAN packets arriving from said

17   source router using the the same encryption algorithms and one or more

18   predetermined keys which were used to encrypt the packets at the location from

19   which they were sent;

20   a source router having an input coupled to said second port of said firewall

21   circuit either directly or by a local area network connection, and having a channel

22   service unit having an output coupled to said dedicated data path, said channel

23   service unit functioning to convert digital data packets received from said firewall

24   circuit into signals suitable for transmission over whatever type of transmission

25   medium is selected for said dedicated data path, and for converting signals received

26   from said dedicated data path into data packets, said source router for transmitting

27   both AlterWAN and non AlterWAN packets over said dedicated data path to said

28   specially selected first participating ISX/ISP provider where AlterWAN packets will be

29   routed via said private tunnel and specially seleted ISX/ISP providers to their

30   destination and non AlterWAN packets will be routed along paths on the internet

31   other than said private tunnel.

32

1   4. (Cancelled) A method of designing and implementing a wide area network using

2   the internet as a backbone, comprising the steps:

3   ~~1) selecting source and destination sites that have devices that need to be~~
4   ~~connected by a wide area network;~~
5   ~~2) examining the ISX/ISP internet service providers that exist between said~~
6   ~~source and destination sites and selecting two or more of such ISX/ISP providers~~
7   ~~through which data passing between said source and destination sites will be routed,~~
8   ~~said selection being based upon how many hops the routers at those sites will cause~~
9   ~~packets travelling between said source and destination sites to take and whether the~~
10   ~~average available bandwidth of the data paths along which the packets travelling~~
11   ~~between said source and destination sites will travel is substantially greater than the~~
12   ~~worst case bandwidth consumption of traffic between said source and destination~~
13   ~~sites;~~
14   ~~3) coupling a source firewall to the devices at said source site and~~
15   ~~configuring said firewall to examine the destination addresses of packets received~~
16   ~~from said devices at said source site and encapsulate each packet addressed to any~~
17   ~~device at said destination site in an internet protocol packet, hereafter referred to as~~
18   ~~an AlterWAN packet, said AlterWAN packet having as its destination address the~~
19   ~~address of an untrusted port of a destination firewall at said destination site and~~
20   ~~having the original IP packet as its payload, said source firewall being configured to~~
21   ~~encrypt the payload portions of all said AlterWAN packets using a predetermined~~
22   ~~encryption algorithm and one or more encryption keys but not to encapsulate or~~
23   ~~encrypt the payload portions of any packets received from said devices at said~~
24   ~~source site which are not addressed to any device at said destination site, and~~
25   ~~configuring said source firewall to recognize any incoming AlterWAN packets which~~
26   ~~have as their destination addresses the IP address of the untrusted side of said~~
27   ~~source firewall and to strip off the AlterWAN packet headers and decrypt the payload~~
28   ~~portion of each said AlterWAN packet to recover the original IP packet transmitted~~
29   ~~from said destination site using the same encryption algorithm and the same~~
30   ~~encryption key or keys used to encrypt the payload portions of said AlterWAN~~
31   ~~packets at said destination site and for outputting said recovered the original IP~~
32   ~~packet to said devices at said source site, said source firewall having an untrusted~~
33   ~~port;~~
34   ~~4) coupling a source router to receive said encrypted and non encrypted~~
35   ~~packets from said untrusted port of said source firewall and to convert them in a~~
36   ~~channel service unit to signals suitable for transmission over a first dedicated local~~
37   ~~loop connection;~~

38 ———— 5) contracting to establish said first dedicated local loop connection between

39 the output of said source router at which said signals appear and a first participating

40 ISX/ISP provider in the group of ISX/ISP providers selected in step 2;

41 ———— 6) providing a destination router at said destination site having a channel

42 service unit which functions to receive from a second dedicated local loop connection

43 downstream signals encoding both encrypted AlterWAN packet and conventional IP

44 packets and converting said signals back into the original digital packet form and

45 outputting the recovered downstream packets at a firewall port, and said destination

46 router configured to receive upstream AlterWAN and conventional packets and

47 convert them into signals suitable for transmission on said second dedicated data

48 path coupling said destination router to an endpoint participating ISX/ISP provider in

49 the group of ISX/ISP providers selected in step 2 and transmitting said signals on

50 said second dedicated local loop connection;

51 ———— 7) contracting to provide a second dedicated local loop connection

52 connecting the input of said destination router to said endpoint participating ISX/ISP

53 provider, said second dedicated local loop connection having sufficiently high

54 bandwidth to handle the worst case traffic volume;

55 ———— 8) providing a destination firewall having an untrusted port having an IP

56 address coupled to said firewall port of said destination router to receive said

57 recovered digital packets, and configuring said destination firewall to recognize as

58 AlterWAN packets incoming recovered packets having as their destination address

59 the IP address of said destination firewall untrusted input port and to strip off the

60 AlterWAN packet header and decrypt the payload portion of said AlterWAN packet

61 using the same encryption algorithm and encryption key or keys that were used to

62 encrypt the packet at said source firewall, and configuring said destination firewall to

63 output the decrypted packets at an output coupled to devices at said destination

64 site, and configuring said destination firewall to examine the destination addresses of

65 upstream IP packets received from said devices at said destination site and

66 encapsulate each upstream IP packet addressed to any device at said source site in

67 another IP packet, hereafter referred to as an AlterWAN packet, said AlterWAN

68 packet having as its destination address the IP address of an untrusted port of said

69 source firewall at said source site and having the original IP packet as its payload,

70 said destination firewall being configured to encrypt the payload portions of all said

71 AlterWAN packets using a predetermined encryption algorithm and one or more

72 encryption keys but not to encapsulate or encrypt the payload portions of any IP

73 ~~packets received from said devices at said destination site which are not addressed~~
74 ~~to any device at said source site (hereafter referred to as conventional packets), and~~
75 ~~said destination firewall configured to transmit said encrypted AlterWAN packets and~~
76 ~~said conventional packets to said destination router via said untrusted port.~~

1 5. (Cancelled) ~~A wide area network using the internet as a backbone, comprising:~~
2 ~~a first dedicated line coupled to a first participating ISX/ISP provider of~~
3 ~~internet access;~~
4 ~~a source router having a channel service unit having an output coupled to~~
5 ~~said first dedicated line;~~
6 ~~a source firewall circuit having a first port for coupling directly or through a~~
7 ~~local area network to a first device for which communication over said wide area~~
8 ~~network (hereafter WAN) is desired, and having a WAN interface coupled to said~~
9 ~~source router directly or through a local area network, said source firewall functioning~~
10 ~~to encrypt the payloads of downstream WAN packets being transmitted via the WAN~~
11 ~~interface to said source router using a first encryption method having a first set of~~
12 ~~user definable keys which may be only one key, and for decrypting the payloads of~~
13 ~~any incoming upstream WAN packets arriving from said first participating ISX/ISP~~
14 ~~using a second encryption method which is different than said first encryption method~~
15 ~~and a second set of user definable keys which are different than the first set of user~~
16 ~~definable keys were used to encrypt the downstream WAN packets;~~
17 ~~one or more routers of other participating ISX/ISP providers of internet~~
18 ~~services including a router at an endpoint participating ISX/ISP provider, said routers~~
19 ~~functioning to implement a predetermined private tunnel data path coupling a router~~
20 ~~of said first ISX/ISP to a router of said endpoint participating ISX/ISP provider~~
21 ~~through said routers of said participating ISX/ISP providers;~~
22 ~~a destination router including a channel service unit coupled to or part of said~~
23 ~~destination router, said destination router coupled through said channel service unit~~
24 ~~and a second dedicated line to said router of said endpoint ISX/ISP provider;~~
25 ~~a destination firewall circuit having a WAN interface coupled to said~~
26 ~~destination router directly or through a local area network and having a second port~~
27 ~~for coupling directly or through a local area network to a device for which~~
28 ~~communication across said wide area network is desired, said destination firewall~~
29 ~~functioning to encrypt the payloads of upstream WAN packets being transmitted~~
30 ~~through said WAN interface to said destination router for transmission to said source~~

31 ~~router via said private tunnel using the same encryption method and user-definable~~
32 ~~key or keys used by said source firewall to decrypt upstream WAN packets, and for~~
33 ~~decrypting any incoming downstream WAN packets from said source router arriving~~
34 ~~from said destination router via the router of said endpoint participating ISX/ISP~~
35 ~~provider using the same encryption method and encryption key or keys used by said~~
36 ~~source firewall to encrypt downstream WAN packets and transmitting the decrypted~~
37 ~~packets to said second device.~~

1   6. (Currently Amended) A private, secure wide area network <u>using the internet as a</u>
2 <u>backbone</u> between a source site and a destination site ~~using the internet as a backbone~~,
3 comprising:
4   a first dedicated ~~local loop connection providing a~~ signal path to a router of a
5 source ISX/ISP provider of internet access;
6   a source router located at a source site and having a channel service unit having
7 an output coupled to said first dedicated <u>signal path</u> ~~local loop connection~~ <u>and having a</u>
8 <u>routing table which has been configured to recognize AlterWAN packets and always route</u>
9 <u>them over said first dedicated signal path to said source ISX/ISP provider, said AlterWAN</u>
10 <u>packets being packets having as their destination address one of one or more</u>
11 <u>predetermined Internet Protocol addresses assigned to an AlterWAN private tunnel, and</u>
12 <u>AlterWAN private tunnel being a data path through the internet which uses only high</u>
13 <u>bandwidth, low latency data paths between predetermined ISX/ISP provider sites which</u>
14 <u>have been pre-tested to ensure that adequate bandwidth and low latency exists for</u>
15 <u>AlterWAN packets and that AlterWAN packets are always routed at said predetermined</u>
16 <u>ISX/ISP provider site into said AlterWAN private tunnel</u>;
17   a source firewall circuit located at a source site and having a first port for coupling
18 directly or through a local area network to one or more computers or other devices at said
19 source site for which communication over said private, secure wide area network
20 (hereafter WAN) is desired, and having a WAN interface coupled to said source router
21 directly or through a local area network, said source firewall functioning to encapsulate
22 any Internet Protocol packets hereafter IP packets transmitted from said first computer or
23 other device which have a destination Internet Protocol address (hereafter IP address)
24 which is one of a set of <u>"predetermined IP addresses", said "predetermined IP addresses"</u>
25 <u>being</u> IP addresses of computers or other devices at a destination site <u>which are</u>
26 <u>assigned to said private tunnel,</u> said encapsulation being<u> performed on</u> ~~into~~ the payload

27 sections of IP packets having as their destination address one of said "predetermined IP

28 addresses", hereafter referred to as AlterWAN packets ~~the IP address of a firewall at said~~

29 ~~destination site~~ and for encrypting said payload sections of said AlterWAN packets using

30 any encryption method known to a destination firewall at a destination site ~~having a key,~~

31 and transmitting said AlterWAN packets to said source router, ~~where IP packets having as~~

32 ~~their destination address the IP address of a computer or other device at either said~~

33 ~~source site or said destination site and having an encrypted IP packet transmitted from a~~

34 ~~computer or other device at said source site or said destination site as a payload being~~

35 ~~defined and hereafter referred to as AlterWAN packets,~~ but said source firewall for not

36 encapsulating ~~into AlterWAN packets~~ any IP packets transmitted by said first computer or

37 other device which do not have as their destination address one of said "predetermined

38 IP addresses" ~~an IP address which is one of said IP addresses of computers or other~~

39 ~~devices at said destination site~~, and for receiving incoming IP packets from various

40 sources including computers and devices at said destination site via said source router

41 and for recognizing AlterWAN packets among these IP packets on the basis that an

42 AlterWAN packet has one of said "predetermined IP addresses" as its destination

43 address, and decrypting the payloads of said AlterWAN packets ~~using the same~~

44 ~~encryption method and key or keys that were used to encrypt the AlterWAN packets~~ to

45 recover said IP packets that were encapsulated in said AlterWAN packets and

46 transmitting at least said recovered IP packets to said one or more computers or devices

47 at said source site to which said recovered IP packets are addressed;

48 one or more internet data paths coupled to routers of said predetermined ~~other~~

49 ~~participating~~ ISX/ISP providers of internet services, said routers having their routing tables

50 configured to recognize said AlterWAN packets by their destination addresses and to

51 cause said routers to route AlterWAN packets into said AlterWAN private tunnel data

52 path, each ~~besides said source ISX/ISP provider including a router at an endpoint~~

53 ~~participating ISX/ISP provider, said routers of said source and endpoint ISX/ISP providers~~

54 ~~and said other participating ISX/ISP providers functioning to implement a predetermined~~

55 ~~private tunnel data path for said AlterWAN packets coupling a router of said source~~

56 ~~ISX/ISP provider to a router of said endpoint participating ISX/ISP provider through said~~

57 ~~routers of said other participating ISX/ISP providers, said source and endpoint ISX/ISP~~

58 ~~providers and~~ said predetermined ~~other~~ ISX/ISP ~~providers being providers~~ provider being

59 a provider of internet services who has ~~have~~ contracted to provide routing of AlterWAN

60 packets into said AlterWAN private tunnel data path, said AlterWAN private tunnel data

61 path being at least one of said internet data paths which has ~~and who have~~ been pre-

62 tested ~~pretested~~ to verify that said data path does ~~they do~~ in fact provides a low hop

63 count data path having ~~portion of a data path between a said source site and a said~~

64 ~~destination site for said AlterWAN packets~~ with an average available bandwidth along

65 each ~~said~~ portion of said data path travelled by said AlterWAN packets which ~~each~~

66 ~~ISX/ISP provider provides which~~ substantially exceeds the worst case bandwidth

67 consumption of AlterWAN packet traffic between said source site and said destination

68 site;

69 a destination router including a channel service unit coupled to or part of said

70 destination router and having a trusted side output, said destination router coupled

71 through said channel service unit and a second dedicated data path ~~local loop~~

72 ~~connection~~ to ~~said~~ a router of a said participating ~~endpoint~~ ISX/ISP provider, said

73 destination router having its routing tables configured to recognize said AlterWAN packets

74 and route them to said trusted side output;

75 a destination firewall circuit having a WAN interface coupled to said trusted side

76 output of said destination router directly or through a local area network and having a

77 second port for coupling directly or through a local area network to a one or more

78 computers or devices for which communication across said private AlterWAN data path,

79 ~~secure wide area network~~ is desired, said destination firewall functioning to encapsulate

80 into the payload sections of AlterWAN packets IP packets transmitted from said one or

81 more computers or devices at said destination site and having as their destination

82 addresses one of said "predetermined IP addresses" which is an IP address of said one

83 or more computers or devices at said source site, and functioning to encrypt the payloads

84 of said AlterWAN packets and transmit said AlterWAN packets to said destination router,

85 but for not encapsulating into AlterWAN packets any IP packets transmitted from said one

86 or more computers or devices at said destination site which do not have as their

87 destination address one of said "predetermined IP addresses" ~~an IP address of said one~~

88 ~~or more computers or devices at said source site~~, and for receiving IP packets from

89 various sources including said one or more computers or devices at said source site via

90 said destination router, and functioning to recognize AlterWAN packets among said

91 received IP packets and decrypt the payload sections of said AlterWAN packets to

92 recover the original IP packets ~~using the same encryption protocol used by said source~~

93 ~~firewall to encrypt said payload sections of said AlterWAN packets and the same key or~~

94 ~~keys used by said source firewall~~ and transmitting at least the decrypted IP packets

95 recovered from AlterWAN packet to said one or more computers or devices at said

96 destination site.

1　　　　7. (Currently Amended) A process for sending AlterWAN data packets securely between

2　　a computer at a source site and a computer at a destination site so as to implement a <u>private</u>

3　　Wide Area Network <u>(hereafter AlterWAN)</u> between said source and destination sites of a

4　　customer<u>, said AlterWAN</u> using the internet as a backbone but which is private and which only

5　　said customer can use ~~while simultaneously launching non-AlterWAN packets into a normal~~

6　　~~internet traffic routing data path~~, comprising the steps:

7　　　　　　receiving at a source firewall incoming Internet Protocol packets (hereafter IP

8　　　　　packets) from a computer~~s~~ at a source site of a customer, some of said IP packets having

9　　　　　as their destination addresses an Internet Protocol address (hereafter IP address) <u>which</u>

10　　　　<u>is one of one or more IP addresses</u> of ~~a computer~~ <u>one or more computers or other</u>

11　　　　<u>computing devices</u> at a destination site of said customer;

　　　　　　at said source firewall, comparing the destination address in each said received

IP packet to an IP address of a computer at said destination site of said customer, and if

an IP packet has as its destination address the IP address of a computer <u>or other</u>

<u>computing device</u> at said destination site <u>(hereafter referred to as an AlterWAN inner</u>

<u>packet)</u>, concluding said IP packet is an AlterWAN <u>inner</u> packet ~~payload~~ which needs to

be transmitted ~~via a virtual private network over the internet~~ to said computer <u>or other</u>

<u>computing device</u> at said destination site <u>via a high bandwidth, low latency, low hop</u>

<u>count data path using said internet as a backbone and connecting said source site to</u>

<u>said destination site</u> <u>and having an average available bandwidth which exceeds the worst</u>

<u>case bandwidth consumption of packets traveling between said source site and said</u>

<u>destination site (hereafter referred as the AlterWAN data path)</u>, but if said destination

address of said received IP packet is not an IP address of a computer <u>or other computing</u>

<u>device</u> at said destination site, concluding said IP packet is ~~nont~~ an AlterWAN <u>inner</u>

~~payload~~ packet and needs to be routed <u>like</u> ~~as~~ any other IP packet would be routed;

　　　　　　if ~~a~~ <u>said</u> received IP packet is an AlterWAN <u>inner</u> ~~payload~~ packet, encapsulating

said AlterWAN <u>inner</u> ~~payload~~ packet into the payload section of <u>a second</u> ~~an~~ IP packet

having as its destination address the IP address of <u>an untrusted side of</u> a firewall at <u>said</u>

~~the~~ destination <u>site</u> ~~end~~ of said <u>AlterWAN data path</u> ~~virtual private network~~ (hereafter

referred to as <u>composite</u> AlterWAN packet) and encrypting at said source firewall <u>at least</u>

~~the~~ <u>a</u> payload portion of said AlterWAN <u>inner</u> packet using any encryption algorithm <u>which</u>

<u>can be decrypted by said firewall at said destination site</u> ~~having a key which same~~

~~encryption algorithm and key can be used by a firewall at said destination site to recover~~

~~said AlterWAN payload packet~~, and forwarding said <u>composite</u> AlterWAN packet to a

source router;

if a said received IP packet is not an AlterWAN inner payload packet, forwarding said received IP packet which is not an AlterWAN payload packet (hereafter referred to as a non-AlterWAN packet) to said source router without encapsulating said non-AlterWAN packet into an a composite AlterWAN packet;

at said source router, converting both said composite AlterWAN packets and said non-AlterWAN packets into signals suitable for transmission on a dedicated signal path local-loop connection coupling said source router to a specially selected predetermined source participating ISX/ISP provider of internet connectivity and routing services, and transmitting said signals to said specially selected predetermined source participating ISX/ISP provider, said predetermined specially-selected source participating ISX/ISP provider being selected because said provider has available a high bandwidth, low latency, low hop count data path which is part of said AlterWAN data path and also has agreed to route said chomposite AlterWAN packets into said AlterWAN data path and has routers wich either already contain routing statements which will route said AlterWAN packets into said AlterWAN data path or which have been configured to contain such a routing statement or statements. either because their routing tables are such that AlterWAN packets will naturally be routed along high bandwidth, low hop count data paths to next participating ISX/ISP provider in said virtual private network or because the routing tables of the router of said specially selected source participating ISX/ISP provider have been altered to insure that AlterWAN packets get routed along high bandwidth, low hop count data paths to the next ISX/ISP provider along said virtual private network and wherein said source participating ISX/ISP provider and all other participating ISX/ISP providers whose routers route AlterWAN packets have contracted to provide a data path for said AlterWAN packets with an average available bandwidth which exceeds the worst case bandwidth consumption of AlterWAN packets traveling between said source site and said destination site of said customer.

1   8. (Currently amended) An apparatus comprising:
2   a dedicated data path for coupling signals to a specially selected first participating
3   ISX/ISP provider of internet access;
4   a first firewall circuit having a first port for coupling directly or through a local area
5   network to one or more computing devices for which is desired communication over a
6   private wide area network between a customer's source site and destination site using
7   the internet as a backbone is desired, and having a second port, said firewall functioning

8   to use the destination addresses in the headers of each packet received from said one or

9   more computing devices at said source site to distinguish between conventional packets

10   and AlterWAN payload packets, where AlterWAN payload packets are packets having as

11   their destination addresses an address of a computing device ~~addressed to devices~~ at

12   said destination site or said source site, and wherein a computing device ~~computer~~ at

13   said destination site is coupled to a computer ~~computing device~~ at said source site via a

14   second firewall circuit and an AlterWAN data path comprising of a virtual private network

15   tunnel implemented along a high bandwidth, low latency, low hop count data paths

16   through a public wide area network such as the internet terminating at said source site at

17   an untrusted side of said first firewall circuit and terminating at said destination site at an

18   untrusted side of said second firewall circuit, and wherein conventional packets are

19   packets which are not addressed to any computing device ~~devices~~ at said destination

20   site, said first firewall circuit functioning to encapsulate said AlterWAN payload packets in

21   the payload section of AlterWAN packets which have as their destination address the

22   address of said untrusted side of ~~are addressed to~~ said second firewall circuit at said

23   destination end of said virtual private network tunnel, ~~and~~ said first firewall circuit further

24   functioning to encrypt the payloads (AlterWAN payload packet) of AlterWAN packets

25   ~~using one or more predetermined keys and an encryption algorithm~~, and distinguishing

26   ~~said first firewall circuit further functioning to distinguish~~ between incoming AlterWAN

27   packets from said destination site and conventional packets by comparing the destination

28   addresses thereof to the address of said untrusted side of said first firewall circuit and

29   concluding that any incoming packets addressed to said first firewall circuit are AlterWAN

30   packet and all packets addressed to one or more computing devices ~~computers~~ at said

31   source site coupled to said first firewall circuit are conventional packets, and further

32   functioning to decrypt the payload sections of any incoming AlterWAN packets ~~using the~~

33   ~~same encryption algorithm and one or more predetermined keys which were used to~~

34   ~~encrypt the AlterWAN packets~~ so as to recover the encapsulated AlterWAN payload

35   packet;

36   a source router having an input coupled to said second port of said first firewall

37   circuit either directly or by a local area network connection, and having a channel service

38   unit having an output coupled to said dedicated data path, said router and channel

39   service unit functioning to receive said AlterWAN packets and said conventional packets

40   from said first firewall circuit and convert said packets into signals suitable for transmission

41   over whatever type of transmission medium is selected for said dedicated data path, and

42   for converting signals received from said dedicated data path into data packets, said

43 source router for transmitting both AlterWAN packets and conventional packets <u>received</u>
44 <u>from said first firewall</u> over said dedicated data path to said specially selected first
45 participating ISX/ISP provider where said AlterWAN packets will be routed ~~via said virtual~~
46 ~~private network tunnel and specially selected participating ISX/ISP providers~~ <u>via said</u>
47 <u>AlterWAN data path</u> to said second firewall ~~and non-AlterWAN packets will be routed~~
48 ~~along paths on the internet other than said virtual private network tunnel~~ and wherein
49 said <u>AlterWAN data path has</u> ~~first participating ISX/ISP provider and all said other~~
50 ~~ISX/ISP providers are providers who have contracted to and do in fact provide data paths~~
51 ~~for AlterWAN packets which combine to form a low hop count data path with~~ an average
52 available bandwidth which substantially exceeds the worst case bandwidth consumption
53 of AlterWAN packets traveling between said source site and said destination site.

1 9. (Currently amended) A method of designing and implementing a <u>private</u> wide area
2 network using the internet as a backbone <u>carrying data packets between a source site to a</u>
3 <u>destination site hereafter referred to as an AlterWAN data path)</u>, comprising the steps:
4 1) selecting source and destination sites that have computers or other devices
5 (hereafter referred to simply as computers) that need to be connected by a wide area
6 network;
7 2) examining available ISX/ISP internet service providers that can route
8 ~~AlterWAN~~ packets between said source and destination sites and selecting two or more
9 of such ISX/ISP providers as participating ISX/ISP providers including at least a source
10 ISX/ISP provider and a destination ISX/ISP provider through which ~~AlterWAN~~ packet
11 data passing between said source and destination sites will be routed, said selection of
12 said participating ISX/ISP providers being made <u>upon the availability to said participating</u>
13 <u>ISX/ISP providers of one or more high bandwidth, low latency data paths which will form</u>
14 <u>part of said AlterWAN data path, said participating ISX/ISP providers agreeing to route</u>
15 <u>packets travelling between said source site and said destination site (hereafter AlterWAN</u>
16 <u>packets) into said AlterWAN data path and agreeing to allow route statements to be</u>
17 <u>added to their routers to cause AlterWAN packets to always be routed into said AlterWAN</u>
18 <u>data path,</u> ~~so as to minimize the number of hops on the internet the routers at~~
19 ~~participating ISX/ISP providers will cause AlterWAN packets to take while traveling~~
20 ~~between said source and destination sites and so as to~~ <u>said participating ISX/ISP</u>
21 <u>providers also agreeing to manage their portions of said AlterWAN data path so as to</u>
22 guarantee that the average available bandwidth of <u>their portion of said AlterWAN data</u>
23 <u>path</u> ~~the data paths along which said AlterWAN packets traveling between computers at~~

24 ~~said source and destination sites will travel~~ is substantially greater than the worst case

25 bandwidth consumption of <u>AlterWAN packet</u> traffic between said source and destination

26 sites;

27 3) <u>adding route statements to routers of said participating ISX/ISP providers</u>

28 <u>which will to cause AlterWAN packets to always be routed into said AlterWAN data path</u>

29 <u>and</u> pretesting <u>said</u> ~~the~~ ISX/ISP providers selected in step 2 by testing to verify the data

30 path that ~~an~~ AlterWAN packets <u>travel</u> will <u>be a portion of said AlterWAN data path and</u>

31 <u>that performance is adequate;</u> ~~take through the internet to verify that what the~~

32 ~~participating ISX/ISP providers promised to deliver will actually be delivered;~~

33 ~~4) contracting with said participating ISX/ISP providers to provide routing of~~

34 ~~AlterWAN packets so as to minimize the number of hops on the internet said AlterWAN~~

35 ~~packets need to take in traveling between said source and destination sites and so as to~~

36 ~~guarantee that the average available bandwidth along data paths AlterWAN packets~~

37 ~~must traverse to travel between said source and destination sites is substantially greater~~

38 ~~than the worst case bandwidth consumption of traffic between source and destination~~

39 ~~sites, and, if necessary, configuring data in routing tables of said participating ISX/ISP~~

40 ~~providers so as to minimize said number of hops and guarantee said bandwidth~~

41 ~~contracted for when routing AlterWAN packets;~~

42 4 ~~5)~~ contracting to establish <u>and establishing</u> a first dedicated <u>signal path</u> ~~local~~

43 ~~loop connection~~ between the output of a source router at which said signals appear and

44 said source ISX/ISP provider in <u>said</u> ~~the~~ group of <u>participating</u> ISX/ISP providers selected

45 in step 2, said first dedicated <u>signal path</u> ~~local loop connection~~ having sufficiently high

46 bandwidth to handle the worst case traffic volume in AlterWAN packets ~~traveling between~~

47 ~~said source and destination sites~~;

48 5 ~~6)~~ contracting to provide a second dedicated <u>signal path</u> ~~local loop connection~~

49 connecting the input of a destination router to said destination ISX/ISP provider, said

50 second dedicated local loop connection having sufficiently high bandwidth to handle the

51 worst case traffic volume in AlterWAN packets ~~traveling between said source and~~

52 ~~destination sites~~;

53 6 ~~7)~~ coupling an untrusted port of a source firewall/virtual private network circuit

54 (hereafter referred to as the source firewall) to a source router and coupling a trusted port

55 of said source firewall to ~~said~~ <u>one or more computing</u> device or devices at said source site

56 and configuring said source firewall to examine the destination addresses of <u>a first</u>

57 internet Protocol packet~~s~~ (hereafter IP packet~~s~~) received from <u>one of</u> ~~said~~ <u>one or more</u>

58 <u>computing</u> devices at said source site and <u>encapsulating</u> ~~encapsulate~~ each <u>first</u> IP packet

59   having as its destination address and address which is a ~~the~~ Internet Protocol address

60   (hereafter IP address) of any computing device at said destination site as a payload

61   portion in a second IP packet, said second IP packet hereafter referred to as an

62   AlterWAN packet, said AlterWAN packet having as its destination address the IP address

63   of an untrusted port of a destination firewall/virtual private network circuit (hereafter

64   referred to as the destination firewall) at said destination site and having an encrypted

65   version of at least the payload section of said first ~~the original~~ IP packet as its payload,

66   said source firewall being configured to recognize non AlterWAN packets and with

67   portions of said AlterWAN packet other than said payload section being referred to herein

68   as an AlterWAN packet header, ~~said source firewall also being configured to encrypt the~~

69   ~~payload portions of all said AlterWAN packets using a predetermined encryption algorithm~~

70   ~~and one or more encryption keys but~~ not to encapsulate or encrypt the payload portions

71   of any non AlterWAN packets received from one or mor of said devices at said source site

72   which do not have as their destination address an ~~the~~ IP address of any device at said

73   destination site ~~(hereafter referred to as non AlterWAN packets)~~, and configuring said

74   source firewall to screen incoming IP packets from said destination firewall so as to

75   recognize any incoming AlterWAN packets which have as their destination addresses the

76   IP address of the untrusted port of said source firewall and to strip off said ~~the~~ AlterWAN

77   packet headers and decrypt a ~~the~~ payload portion of each said incoming AlterWAN

78   packet to recover the original IP packet transmitted from said destination firewall ~~using the~~

79   ~~same encryption algorithm and the same encryption key or keys used to encrypt the~~

80   ~~payload portions of said AlterWAN packets when they were transmitted from said~~

81   ~~destination firewall~~ so as to recover the original IP packet transmitted to said destination

82   firewall by a computer at said destination site, and for outputting said recovered original

83   IP packet to said device or devices at said source site having the IP address which is the

84   destination address of said original IP packet;

85   7 ~~8)~~ coupling a source router to receive said ~~encrypted~~ AlterWAN packets and

86   ~~non-encrypted~~ non-AlterWAN packets from said ~~untrusted port of said~~ source firewall and

87   to convert said AlterWAN and non-AlterWAN packets in a channel service unit to signals

88   suitable for transmission over said first dedicated signal path ~~local loop connection~~ to said

89   source ISX/ISP provider;

90   8 ~~9)~~ providing a destination router at said destination site having a firewall port

91   coupled to an ~~said~~ untrusted port of said destination firewall and having a channel

92   service unit coupled to said destination ISX/ISP provider via said second dedicated signal

93   path ~~local loop connection~~ and configuring said destination router ~~which is configured~~ to

94   receive from said second dedicated <u>signal path</u> local loop connection downstream signals

95   encoding both encrypted AlterWAN packets and conventional non AlterWAN IP packets

96   and <u>convert</u> converting said signals back into the original digital IP packet form<u>,</u> and

97   configuring said destination router to output said recovered downstream IP packets at

98   said firewall port coupled to said untrusted port of said destination firewall, and

99   <u>configuring</u> said destination router configured to receive upstream AlterWAN packets and

100   conventional non AlterWAN packets and convert both types of said packets into signals

101   suitable for transmission on said second dedicated <u>signal path</u> local loop connection

102   coupling said destination router to said participating destination ISX/ISP provider in <u>said</u>

103   the group of participating ISX/ISP providers selected in step 2, and <u>configuring said</u>

104   <u>router to transmit</u> transmitting said signals on said second dedicated <u>signal path</u> local

105   loop connection;

106   <u>9</u> 10) providing <u>said</u> a destination firewall having an untrusted port coupled to

107   said firewall port of said destination router so as to receive said recovered digital IP

108   packets, and configuring said destination firewall to recognize as AlterWAN packets

109   incoming recovered IP packets having as their destination address the IP address of said

110   destination firewall untrusted port and further <u>configuring said destination firewall</u>

111   configured to strip off <u>said</u> the AlterWAN packet header of each said AlterWAN packet

112   and<u>, as to each AlterWAN packet,</u> decrypt<u>ing a</u> the payload portion of each said

113   AlterWAN packet using the same encryption algorithm and encryption key or keys that

114   were used to encrypt the AlterWAN packet at said source firewall so as to recover <u>said</u>

115   <u>first</u> the original IP packet <u>which</u> encapsulated in <u>said</u> each AlterWAN packet, and

116   configuring said destination firewall to output <u>said first IP packet recovered from said</u>

117   <u>AlterWAN packet by said decryption process</u> the decrypted original and output each said

118   <u>first</u> IP packets <u>so recovered</u> at an output coupled to <u>one or more computing</u> a device or

119   devices at said destination site, and configuring said destination firewall to examine the

120   destination addresses of upstream <u>first</u> IP packets received from <u>said one or more</u>

121   <u>computing</u> a device or devices at said destination site and encapsulate each upstream

122   <u>first</u> IP packet addressed to any computer or other <u>computing</u> device at said source site

123   as <u>a</u> the payload portion of <u>in a second</u> another IP packet, hereafter referred to as an

124   upstream AlterWAN packet (an AlterWAN packet traveling from said destination site

125   toward said source site), <u>each</u> said <u>upstream</u> AlterWAN packet having as its destination

126   address the IP address of said untrusted port of said source firewall at said source site

127   and <u>a first</u> having the original IP packet as its payload, <u>and further configuring said</u> said

128   destination firewall being configured to encrypt the payload portions of <u>each</u> all said

129   upstream AlterWAN packets using a predetermined encryption algorithm and one or more

130   encryption keys but not to encapsulate or encrypt the payload portions of any non

131   AlterWAN IP packets received from said <u>one or more computing device or</u> devices at said

132   destination site<u>, said non AlterWAN IP packets being those IP packets</u> which do not have

133   as their destination addresses an IP address of any device at said source site (hereafter

134   referred to as conventional non AlterWAN packets), and <u>configuring</u> said destination

135   firewall configured to transmit said encrypted upstream AlterWAN packets and said

136   conventional non AlterWAN packets to said destination router via said untrusted port.

1   10. (Currently amended) A private wide area network connecting a customer source site

2   to a customer destination site and using the internet as a backbone, comprising:

3   a first dedicated data path coupled to a first participating ISX/ISP provider of

4   internet access;

5   a source router having a channel service unit having an output coupled to said

6   first dedicated data path <u>and configured with route statements that recognize IP packets</u>

7   <u>addressed to the untrusted side of a destination firewall at said customer destination site</u>

8   <u>(hereafter outgoing AlterWAN packets) and cause said outgoing AlterWAN packets to be</u>

9   <u>routed into an AlterWAN data path, wherein said AlterWAN data path is a high</u>

10   <u>bandwidth, low latency data path from said customer source site to said customer</u>

11   <u>destination site and back having an average available bandwidth that exceeds the worst</u>

12   <u>case bandwidth consumption of AlterWAN packet traffic between said source and</u>

13   <u>destination sites</u>;

14   a source firewall circuit having a first port for coupling directly or through a local

15   area network to one or more devices at a customer source site, and having an untrusted

16   port coupled to said source router directly or through a local area network, said untrusted

17   port of said source firewall having an Internet Protocol address (hereafter IP address),

18   said source firewall functioning to receive Internet Protocol packets (hereafter IP packets)

19   from said one or more devices at said customer source site which are addressed to one

20   or more devices at a customer destination site (hereafter AlterWAN payload packets) and

21   other IP packets addressed to other locations on the internet (hereafter conventional IP

22   packets), and for encapsulating said AlterWAN payload packets as the payload sections

23   of <u>outgoign AlterWAN</u> IP packets <u>which have as their destination addresses the</u>

24   addressed to an IP address of an untrusted port of a destination firewall at said customer

25   destination site (hereafter outgoing AlterWAN packets) and functioning to encrypt the

26   payloads of said outgoing AlterWAN packets using a first encryption method known to a

27 ~~destination firewall and using a key or key known to said destination firewall and which~~

28 ~~may be user definable~~, and for receiving incoming IP packets and comparing the

29 destination addresses of said incoming IP packets to said IP address of said untrusted

30 port of said source firewall circuit <u>any said incoming IP packet having as its destination</u>

31 <u>address the IP address of said untrusted port of said source firewall being a incoming</u>

32 <u>AlterWAN packet, each said incomimg AlterWAN packet encapsulating as its payload</u>

33 <u>section a AlterWAN payload packet</u>, and decrypting the payload sections of any

34 incoming ~~IP~~ <u>AlterWAN</u> packets ~~having as their destination address the IP address of said~~

35 ~~untrusted port of said source firewall circuit (hereafter incoming AlterWAN packets) using~~

36 ~~whatever encryption method and key or keys which were used to encrypt them~~ so as to

37 recover the encapsulated AlterWAN payload packet from each incoming AlterWAN

38 packet, and transmitting each recovered AlterWAN payload packet to a device at said

39 customer source site to which said AlterWAN payload packet is addressed;

40 one or more routers of ~~other~~ participating ISX/ISP providers of internet services

41 including a router at an endpoint participating ISX/ISP provider, said routers of said

42 ISX/ISP providers functioning to implement <u>said AlterWAN data path as</u> a <u>high</u>

43 <u>bandwidth, low latency,</u> low hop count data path <u>having an average available bandwidth</u>

44 <u>that exceeds the worst case bandwidth consumed by incoming and outgoing AlterWAN</u>

45 <u>packets travelling between said source and destination sites and configured to recognize</u>

46 <u>said incoming and outgoing AlterWAN packets by their destination addresses and route</u>

47 <u>them into said AlterWAN data path,</u> ~~in the form of a virtual private network tunnel through~~

48 ~~the internet coupling one or more devices at said customer source site to one or more~~

49 ~~computers at said customer destination site, said low hop count data path having an~~

50 ~~average available bandwidth which is substantially greater than the worst case bandwidth~~

51 ~~consumption of AlterWAN packets traveling between said customer source site and said~~

52 ~~customer destination site;~~

53 a destination router including a channel service unit coupled to or part of said

54 destination router, said destination router coupled through said channel service unit and

55 a second dedicated datapath to said router of said endpoint participating ISX/ISP

56 provider <u>and configured to recognize said outgoing AlterWAN packets arriving from said</u>

57 <u>endpoint participating ISX/ISP provider which have travelled from said source firewall via</u>

58 <u>said AlterWAN data path and route them to said destination firewall, and configured to</u>

59 <u>recognize said incoming AlterWAN packets from said destination firewall circuit and route</u>

60 <u>them to said endpoint participating ISX/ISP provider;</u>

61 ~~a~~ <u>said</u> destination firewall circuit having an untrusted port having an IP address to

62   which said outgoing AlterWAN packets are addressed, said untrusted port coupled to

63   said destination router directly or through a local area network and having a second port

64   for coupling directly or through a local area network to one or more devices at said

65   customer destination site, said destination firewall circuit <u>configured so as</u> ~~functioning~~ to

66   receive IP packets from said one or more devices at said customer destination site which

67   are addressed to one or more devices at said customer source site (hereafter AlterWAN

68   payload packets) and functioning to receive other conventional IP packets <u>not addresed</u>

69   <u>to any of the said devices at said customer source site</u>, and for encapsulating said

70   AlterWAN payload packets as the payload sections of AlterWAN packets addressed to

71   said IP address of an untrusted port of said source firewall circuit at said customer source

72   site (hereafter <u>incoming</u> ~~outgoing~~ AlterWAN packets) and functioning to encrypt the

73   payloads of said <u>incoming</u> ~~outgoing~~ AlterWAN packets ~~using an encryption method~~

74   ~~known to said source firewall and a key or keys known to said source firewall~~ and for

75   receiving incoming <u>AlterWAN</u> ~~IP~~ packets and comparing the destination addresses of said

76   incoming <u>AlterWAN</u> ~~IP~~ packets to said IP address of said untrusted port of said

77   destination firewall circuit, and decrypting the payload sections of any incoming

78   <u>AlterWAN</u> ~~IP~~ packets having as their destination address the IP address of said

79   untrusted port of said destination firewall circuit ~~(hereafter incoming AlterWAN packets)~~

80   ~~using whatever encryption method and key or keys which were used to encrypt said~~

81   ~~incoming AlterWAN packets~~ so as to recover the encapsulated AlterWAN payload packet

82   from each incoming AlterWAN packet, and transmitting each recovered AlterWAN payload

83   packet to the device to which it is addressed at said customer destination site.

Please add the following new claims:

1   11. (new) A method of doing business to establish a private bidirectional wide area

2 network between a source site and a destination site using the internet as a backbone,

3 comprising the steps:

4   connecting one or more computing devices at a source site to a firewall and

5   source router and obtaining a known IP address for each computing device at said

6   source site;

7   connecting one or more computing devices at a destination site to a firewall and

8   destination router and obtaining a known IP address for each computing device at said

9   destination site;

10   selecting one or more participating ISX/ISP internet service providers which have

11   one or more high bandwidth, low latency, low hop count data paths that can be used as

12   at least part of a high bandwidth, low latency, low hop count data path for transmission of
13   AlterWAN data packets between said source site and said destination site (hereafter
14   referred to as the AlterWAN data path), and making agreements with said participating
15   ISX/ISP internet service providers to always route AlterWAN packets into said AlterWAN
16   data path such that said AlterWAN data packets will only travel on AlterWAN data path,
17   wherein said AlterWAN packets are defined as packets which contain as a destination
18   address one of said known IP addresses of computing devices at said source site or said
19   destination site, and ensuring that said routing tables of routers of said one or more
20   participating ISX/ISP internet service providers either already contain routing statements
21   that will cause AlterWAN packets to be routed into said AlterWAN data path or are
22   modified to contain such route statements;
23   connecting said source router and said destination router to one of said
24   participating ISX/ISP internet service providers through dedicated high bandwidth, low
25   latency data paths.

1   12. [new] A method comprising:
2   generating an Internet Protocol data packet (hereafter IP packet) having as its
3   destination address an Internet Protocol address assigned to a computing device at the
4   other end of a private, wide area network using the internet as a backbone (hereafter
5   referred to as an AlterWAN private tunnel);
6   encrypting a payload portion of said IP packet to generate an encrypted IP
7   packet;
8   generating a composite AlterWAN packet by encapsulating said encrypted IP
9   packet in another IP packet having as its destination address an IP address of an
10   untrusted side of a firewall which is at a destination site which is part of said AlterWAN
11   private tunnel; and
12   routing said composite AlterWAN packet using a source router whose routing
13   table has been configured to include a routing statement which recognizes said
14   destination address of said composite AlterWAN packet and routes said composite
15   AlterWAN packet via a dedicated data path to an AlterWAN data path, said AlterWAN
16   data path being defined as a high bandwidth, low latency, low hop count data path
17   provided by one or more participating ISX/ISP internet service providers that links said
18   source site and said destination site of said AlterWAN private tunnel, each participating
19   ISX/ISP internet service provider being one which has been selected as having at least
20   one high bandwidth, low latency, low hop count data path which can be used to transmit

21 said composite AlterWAN data packet either from said source site to said destination site

22 or to another participating ISX/ISP internet service provider and which has routers which

23 either already contain or which are configured to contain predetermined routing

24 statements when said participating ISX/ISP agrees to provide routing services as part of

25 said AlterWAN data path, said predetermined routing statements being ones which will

26 recognize said IP destination address of each said composite AlterWAN data packets

27 and cause said composite AlterWAN packets to be routed into said AlterWAN data path.

1   13. [new] A method comprising:

2   receiving composite AlterWAN packet comprised of an encapsulating IP packet

3   having as its destination address an Internet Protocol address assigned to a firewall at

4   said destination site and using said Internet Protocol address assigned to said firewall in

5   the destination address field of said encapsulating IP packet to recognize said packet as

6   a composite AlterWAN packet, said encapsulating IP packet including at its payload an

7   encrypted IP packet having as its destination address an Internet Protocol address of a

8   computing device at said destination site, said destination site being at an end of a

9   private, wide area network using the internet as a backbone (hereafter referred to as an

10 AlterWAN private tunnel) and reacting to recognition of said received packet as an

11 AlterWAN composite packet by routing said composite AlterWAN packet to a firewall;

12 in said firewall, decrypting a payload portion of said encrypted IP packet to

13 generate a recovered IP packet;

14 routing said recovered IP packet to a computing device to which said recovered

15 IP packet is addressed.

1   14. [new] A method of doing business comprising:

2   selecting one or more participating ISX/ISP internet service providers

3   which have one or more high bandwidth, low latency, low hop count data paths

4   that can be used as at least part of a high bandwidth, low latency, low hop count

5   data path for transmission of composite AlterWAN data packets between a source

6   site and a destination site of a private wide area network using the internet as a

7   backbone (hereafter referred to as the AlterWAN data path), where composite

8   AlterWAN data packets are defined as internet protocol packets (hereafter the

9   outer packet) which encapsulate other internet protocol packets (hereafter the

10 inner packet), said inner packet having as its destination address the IP address

11 of a computing device at one end of said AlterWAN data path and at least the

12   payload section of said inner packet being encrypted, said outer packet having

13   as its destination address an IP address of an untrusted side of a firewall at the

14   same end of said AlterWAN data path as said computing device which has as its

15   IP address said destination address of said inner packet;

16   making agreements with said participating ISX/ISP internet service

17   providers to always route composite AlterWAN packets into said AlterWAN data

18   path such that said composite AlterWAN data packets will only travel on said

19   AlterWAN data path;

20   ensuring that said routing tables of routers of said one or more

21   participating ISX/ISP internet service providers either already contain routing

22   statements that will cause said composite AlterWAN data packets to be

23   recognized and routed into said AlterWAN data path or are modified to contain

24   such route statements.

1   15. [new] A method of doing business comprising:

2   selecting one or more participating ISX/ISP internet service providers

3   which have one or more high bandwidth, low latency, low hop count data paths

4   that can be used as at least part of a high bandwidth, low latency, low hop count

5   data path for transmission of AlterWAN data packets between a source site and a

6   destination site of a wide area network using the internet as a backbone

7   (hereafter referred to as the AlterWAN data path), where AlterWAN data packets

8   are defined as internet protocol packets which contain as a destination address

9   one of said known IP addresses of computing devices at said source site or said

10   destination site;

11   making agreements with said participating ISX/ISP internet service

12   providers to always route said AlterWAN packets into said AlterWAN data path

13   such that said AlterWAN data packets will only travel on said AlterWAN data path;

14   ensuring that said routing tables of routers of said one or more

15   participating ISX/ISP internet service providers either already contain routing

16   statements that will cause said AlterWAN data packets to be recognized and

17   routed into said AlterWAN data path or are modified to contain such route

18   statements.

1   16. [new] A method of operating a router at an ISX/ISP comprising the steps:

2   using said router to recognize AlterWAN data packets where AlterWAN data

3   packets are defined as internet protocol packets which contain as a destination address

4   one of one or more known IP addresses of computing devices at a source site or a

5   destination site of a wide area network using the internet as a backbone;

6   looking up routing statements that are applicable to said AlterWAN data packets

7   and using said routing statements to route said AlterWAN data packets into a high

8   bandwidth, low latency, low hop count data path coupling said soure site to said

9   destination site.

1   17. [new] A method of operating a router at an ISX/ISP comprising the steps:

2   using said router to recognize composite AlterWAN data packets where composite

3   AlterWAN data packets are defined as internet protocol packets (hereafter the outer

4   packet) which encapsulate other internet protocol packets (hereafter the inner packet),

5   said inner packet having as its destination address one of one or more known IP

6   addresses of computing devices at a source site or a destination site of a wide area

7   network using the internet as a backbone and at least the payload section of said inner

8   packet being encrypted, said outer packet having as its destination address an IP

9   address of an untrusted side of a firewall at the same end of said AlterWAN data path as

10   said computing device which has as its IP address said destination address of said inner

11   packet;

12   looking up routing statements that are applicable to said composite AlterWAN

13   data packets and using said routing statements to route said composite AlterWAN data

14   packets into a high bandwidth, low latency, low hop count data path coupling said soure

15   site to said destination site.

1   18. [new] A router at an ISX/ISP which is part of a private wide area network using the

2   internet as a backbone, said router being conventional except that said router is coupled to a

3   high bandwidth, low latency, low hop count data path and has been configured to contain

4   routing statements that cause AlterWAN data packets to be recognized and routed into said high

5   bandwidth, low latency, low hop count data path, where AlterWAN data packets are defined as

6   internet protocol packets which contain as a destination address one of one or more known IP

7   addresses of computing devices at a source site or a destination site of a wide area network

8   using the internet as a backbone.

1   19. [new] A router at an ISX/ISP which is part of a private wide area network using the

2   internet as a backbone, said router being conventional except that said router is coupled to a

3   high bandwidth, low latency, low hop count data path and has been configured to contain

4   routing statements that cause composite AlterWAN data packets to be recognized and routed

5   into said high bandwidth, low latency, low hop count data path, where composite AlterWAN data

6   packets are defined as internet protocol packets (hereafter the outer packet) which encapsulate

7   other internet protocol packets (hereafter the inner packet), said inner packet having as its

8   destination address one of one or more known IP addresses of computing devices at a source

9   site or a destination site of a wide area network using the internet as a backbone and at least the

10   payload section of said inner packet being encrypted, said outer packet having as its destination

11   address an IP address of an untrusted side of a firewall at the same end of said AlterWAN data

12   path as said computing device which has as its IP address said destination address of said inner

13   packet.